STATE OF WEST VIRGINIA
OFFICE OF THE ATTORNEY GENERAL
DARRELL V. MCGRAW, JR.
CONSUMER PROTECTION DIVISION
1-800-368-8808 or 304-558-8986

Press Release

June 27, 2006

FOR IMMEDIATE RELEASE
CONTACT: CHARLI FULTON
304-558-8986
800-368-8808

NEW SECURITY BREACHES EXPOSE WEST VIRGINIA RESIDENTS TO RISK OF IDENTITY THEFT

On Saturday, June 24, employees of Thomas Memorial Hospital and St. Francis Hospital received a disturbing letter from Medical Excess, LLC, a company most of them had not heard of before. The letter, dated "June 2006," stated that there was a break-in recently at a regional Medical Excess office. A camera, two laptop computers, and a file server were stolen. The file server that was stolen, from a locked room, contained individual names with corresponding Social Security numbers and birth dates. According to the letter, medical and disability information was also stored on the server for a small percentage of the persons. These materials were included in files submitted by insurance brokers and group insurance plans applying for excess insurance. Medical Excess reported the break-in to law enforcement authorities, but the missing items have not been recovered. The letter advised the recipient to watch for any unusual activity on credit card accounts or suspicious items on bills for the next two years. The letter states that the company will provide certain services for persons who notice unusual activity on their accounts and suspect identity theft.

What the letter did not say was that the break-in occurred on March 31 – two and a half months before Medical Excess sent the letter to West Virginia residents. Personal information on more than 900,000 persons was compromised by the security breach. Medical Excess, LLC, located in South Coast Metro, California, is a medical underwriter that provides stop loss medical insurance and other excess insurance coverage. Medical stop loss insurance provides protection against catastrophic or unpredictable losses. It is typically purchased by employers who have self-funded employee benefit plans. This type of insurance provides coverage for losses that exceed deductibles and generally covers catastrophic illnesses. The persons who received the letter from Medical Excess are persons whose employers provide some type of insurance coverage through Medical Excess.

Earlier this month other West Virginia residents received notification of a security breach from Humana. The Humana letter, dated June 2, 2006, stated that a Humana employee used a hotel's business services computer for business purposes, which resulted in some Humana Medicare members' information to be stored in a temporary file on a computer that was available for use by hotel guests. The information included the name, address, telephone number, member identification number, and Social Security number of each affected person. Humana agreed to provide a free credit monitoring service from Equifax for approximately 17,000 affected persons who enroll before September 1, 2006.

The Attorney General's Consumer Protection Division receives many consumer requests for information about how to protect themselves from identity theft as a result of security breaches. The Division recommends that consumers (1) order their credit reports from all three major credit reporting agencies and check them for any suspicious activity, (2) place fraud alerts on their credit reports, and (3) take advantage of any free opportunities to participate in free credit monitoring programs.

Under the 2003 amendments to the federal Fair Credit Reporting Act, consumers may place an initial "fraud alert" on their credit reports for 90 days. During this period, the credit reporting agency must display an alert which notifies all users that the consumer may be a victim of fraud, including identity theft. After 90 days, however, the consumer must submit a qualifying identity theft report from a law enforcement agency in order to obtain an extended fraud alert. An extended alert, which can last up to seven years, requires all users of a consumer credit report to verify the consumer's identity by telephone before proceeding with any credit transaction. Unfortunately, many consumers have difficulty obtaining an extended alert because law

enforcement agencies sometimes refuse to take such reports.

Many states have passed laws providing additional safeguards to prevent or remedy the effects of data security breaches. To date, 23 states have enacted security breach notification and/or security freeze laws. Security breach notification laws require businesses and public institutions to notify persons of any breach of security of computer information systems in which unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Security freeze laws allow consumers to place "security freezes" on their credit reports, thereby giving the consumer control over who will receive a copy of his or her credit report. This makes it nearly impossible for criminals to use stolen information to open an account in the consumer's name.

West Virginia consumers have no such legal protection: they have no right to be notified of security breaches that affect them and no right to freeze their credit reports. Attorney General McGraw proposed a security breach notification law and a security freeze law 2006 legislative session, but neither passed. "Since June 1, 2006, nearly two million Americans have had their personal information stolen because of a security breach. Nearly 89 million Americans have been affected by security breaches in the past 18 months. It is well past the time for laws to be enacted to allow private citizens to lock the door on their personal information before they are the victims of theft," McGraw said.

For more information or to file a complaint, please contact the Attorney General's Consumer Protection Division. Call 1-800-368-8808, write to P.O. Box 1789, Charleston, WV 25326-1789, or by downloading a complaint form from this site.

For a chronology of data security breaches, go to http://www.privacyrights.org/ar/ChronDataBreaches.htm.
For more information about the Model State Clean Credit and Identity Theft Protection Act, go to www.financialprivacynow.org and click on "Learn More" or contact Consumers Union at 1535 Mission Street, San Francisco, CA 94102 or 415-431-6747.

To download and print a complaint form, please click on the ***General Consumer Complaint Form*** link at the top of this page.

###